

Informata për Sigurinë Online: Phishingu

Çka është phishing?

Phishing është emri i cili i është dhënë praktikës së të dërguarit të postave elektronike (e-mailëve) të rastësishme me pretendim se ato vijnë nga një kompani e vërtetë e cila operon në Internet, në përpjekje për të mashtruar konsumatorët e asaj kompanie duke shpalosur kështu informatat në ueb faqe false të operuar nga mashtruesit. Këto posta elektronike zakonisht pretendojnë se është e nevojshme të “azhurnohen” ose “verifikohen” informatat e llogarisë së konsumatorit dhe ato nxisin njerëzit që të klikojnë në një vegëz në postën elektronike e cila i dërgon ata në ueb faqen false. Çfarëdo informate e cila futet në ueb faqen false do të merret nga kriminelët për qëllimet e tyre mashtruese.

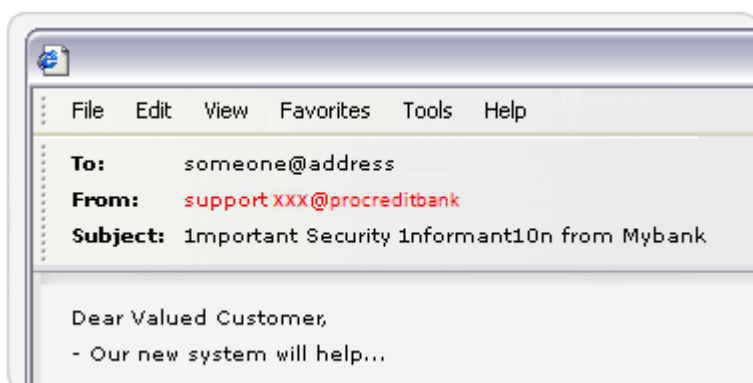
Si mund ta parandalojë që të mos bëhem viktimë e phishing?

Gjëja kryesore është të keni kujdes për të gjitha postat elektronike (e-mailët) të dyshimta dhe të papritura të cilat pranoni, edhe nëse ato duken në shikim të parë se vijnë nga një burim i besueshëm. Këto posta elektronike dërgohen tërësisht në baza të rastësishme duke shpresuar që të arrijë një adresë të postës elektronike aktive të një konsumatori me një llogari në bankën e synuar për sulm.

Edhe pse ProCredit Bank mund t’ju kontaktojë përmes postës elektronike (e-mailit), ProCredit Bank asnjëherë nuk do t’ju kërkojë përmes postës elektronike të futni fjalëkalimin tuaj ose informatat tjera të ndjeshme duke klikuar në një vegëz si dhe duke vizituar një ueb faqe. Rikujtohuni se si banka juaj zakonisht komunikon me ju dhe asnjëherë mos shpalosni fjalëkalimin tuaj të plotë ose ndonjë informatë personale.

Si të dallohet një postë elektronike phishing

1 – Prej kujt është kjo postë elektronike?



Postat elektronike 'phishing' mund të duken sikurse vijnë nga një postë elektronike (e-mail) reale e ProCredit Bank-ës. Fatkeqësisht për shkak të përcaktimit të postës elektronike në Internet, është relativisht e thjeshtë për "phisheret" të krijojnë një hyrje false në fushën "Nga:" ("From:").

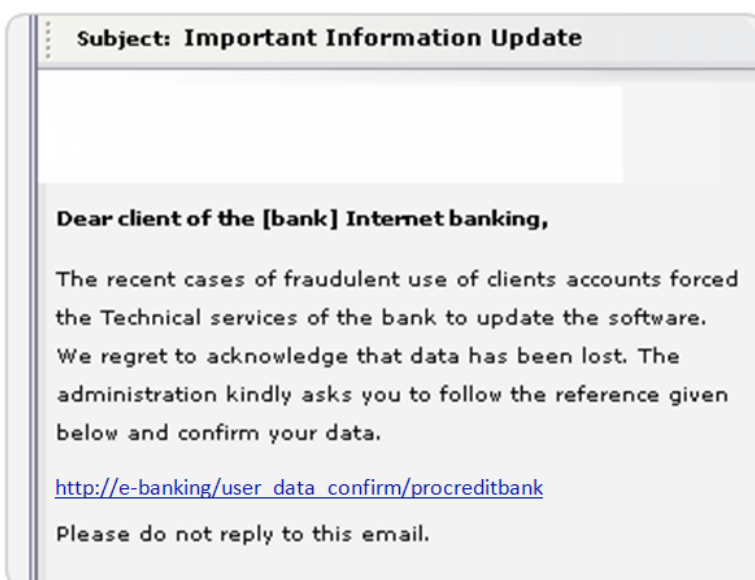
Adresa e postës elektronike e cilat duket në fushën "Nga:" ("From:") të një poste elektronike NUK është vërtetim se ajo vjen nga personi ose organizata e deklaruar në adresën e postës elektronike. Këto posta elektronike nuk janë dërguar duke përdorur sistemet e vetë bankës.

2 – Për kë është kjo postë elektronike?

Postat elektronike (e-mailët) dërgohen rastësisht në një listë të madhe të adresave dhe mashtruesit me siguri se nuk do të dinë emrin tuaj real dhe ndonjë gjë tjetër për ju, dhe do t'ju drejtohen në mënyrë të përgjithshme si "I Nderuari Konsumator i Çmuar", dhe jo duke ju drejtuar me emrin tuaj personal.

3 – Vëreni me kujdes postën elektronike – a duket si "phishing"?

Gjëja e parë për tu mbajtur ndër mend është se banka jonë asnjëherë nuk do t'ju shkruajë për t'ju kërkuar fjalëkalimin ose informatat tjera të ndjeshme përmes postës elektronike (e-mailit). Porosia është e mundur të përmbajë tekste të "paz11konshme" ose "shkroNJa të MëDHa" në fushën e "Titullit:" ("Subject:") (kjo është përpjekje për të anashkaluar softuerin për filtrimin e spamit), si dhe gabime gramatikore dhe të drejtshkrimit.



Shembull i postës elektronike mashtruese

Asnjëherë mos u kyçni në llogarinë e shërbimit bankar online duke klikuar në një vegëz në një poste elektronike. **Gjithnjë** hapeni shfletuesin tuaj të internetit dhe shkruani adresën e ProCredit Bank-ës për shërbime bankare.

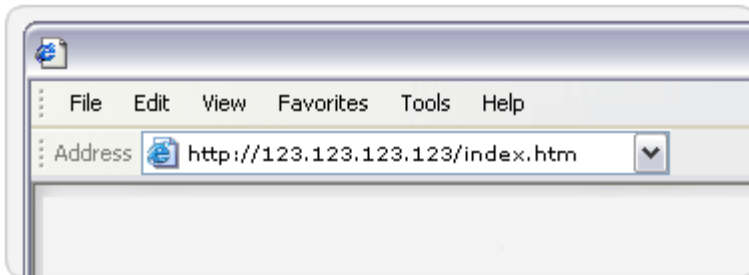
Nëse keni dyshime për vlefshmërinë e një poste elektronike (e-maili) e cila pretendon se vjen nga ProCredit Bank, ju lutemi menjëherë njoftoni ProCredit Bank-ën duke vizituar degën më të afërt, duke kontaktuar këshilltarin tuaj për klient ose duke telefonuar në numrin vijues [**+381-38 / 555-555 apo +386 - 49 / 555-555**]. Ju gjithashtu mund të përcjellni postën elektronike të dyshimtë në adresën vijuese të postës elektronike [**abuse@procreditbank-kos.com**].

4 – Ku shkon ajo vegëz?

Fatkeqësisht, është shumë e lehtë të maskohet destinomi real i një vegëze, ashtu që vegëza e paraqitur dhe gjithçka që paraqitet në rreshtin e statusit të programit tuaj për postë elektronike mund të falsifikohet lehtësisht.

Si të dallohet një ueb faqe Phishing

Çka është adresa e faqes?



Nëse vizitoni një ueb faqe pas klikimit në një vegëz në një postë elektronike (e-mail), ka shumë mënyra për të fshehur lokacionin e vërtetë të asaj ueb faqeje në rreshtin e adresës. Adresa e faqes mund të fillojë me emrin e vërtetë të domenit të faqes, por nuk ka garancion se ajo të dërgon te faqja e vërtetë. Dredhitë tjera përfshijnë përdorimin e adresave numerike, regjistrimin e adresave të ngjashme (si www.mybank-verify.com), madje edhe futjen e rreshtit të adresave të falsifikuar në dritaren e shfletuesit. Shumë nga vegëzat nga këto faqe realisht mund të shkojnë në ueb faqe të vërteta, megjithatë, mos u mashtroni.

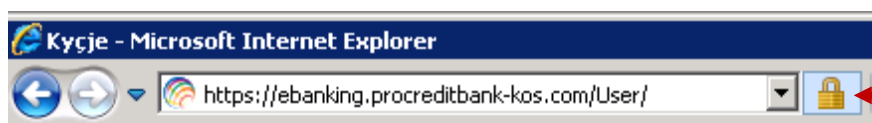
Ju mund të konfirmoni se jeni në ueb faqen zyrtare të sigurt të ProCredit Bank-ës duke krahasuar simbolin e lidhjes së sigurt.

**Shfletuesi i
Internetit 9**



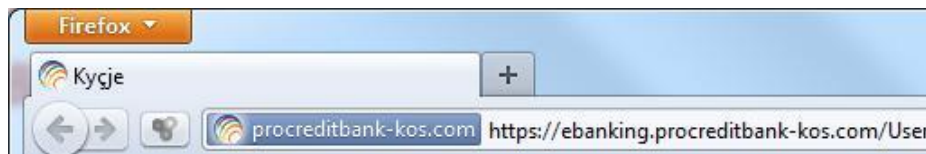
Kliko në këtë ikonë të dryrit dhe do të shiheni Identifikimin e Sigurisë së Ueb Faqes

**Shfletuesi i
Internetit 8**



Kliko në këtë ikonë të dryrit dhe do të shihni Identifikimin e Sigurisë së Ueb Faqes

Firefox 4



Ju mund të kontrolloni **Certifikatën e Sigurisë (Security Certificate)** duke klikuar në drynin i cili paraqitet në shfletuesin tuaj.

Keni kujdes nga dritaret dalëse mashtruese

Në vend të paraqitjes së një faqe tërësisht false, mashtruesit mund të paraqesin ueb faqen e vërtetë në dritaren kryesore të shfletuesit dhe pastaj të vendosin një faqe tjetër dalëse që mbulon shumicën e faqes tjetër. Nëse paraqitet në këtë mënyrë, ju do të jeni në gjendje të

shihni rreshtin e adresës së ueb faqes reale në prapavijë, edhe pse informatat të cilat ju shkruani në dritaren dalëse do të mblidhen nga mashtruesit për përdorim nga ta.

Për tu kyçur në llogarinë tuaj për shërbime bankare online, shkruari vetë adresën në një dritare të re. Adresa reale e ueb faqes së shërbimit bankar online do të fillojë me “https” dhe të përfshijë një dry të vogël në fund të dritares së shfletuesit.